FORM PTO-1390 (REV. 11-2000)	U S DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE	ATTORNEY 'S DOCKET NUMBER PAGA04US

TRANSMITTAL LETTER TO THE UNITED STATES
DESIGNATED/ELECTED OFFICE (DO/EO/US)
CONCERNING A FILING UNDER 35 U.S.C. 371

U S APPLICATION NO (If known, see 37 CFR 1 5

09/890846

INTERNATIONAL APPLICATION NO. PCT/BY99/00011	INTERNATIONAL FILING DATE 8 DEC 1999	PRIORITY DATE CLAIMED 8 DEC 1999

TITLE OF INVENTION
METHOD AND SYSTEM FOR AUTHENTICATION OF ARTICLES

APPLICANT(S) FOR DO/EO/US
MISCHENKO, VALENTIN; HRISHANOVICH, IGOR; MISCHENKO, ANATOLY
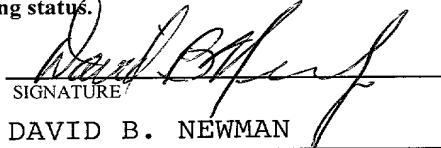
Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. ☒ This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.

2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.

3. ☐ This is an express request to begin national examination procedures (35 U.S.C. 371(f)). The submission must include items (5), (6), (9) and (21) indicated below.

4. ☐ The US has been elected by the expiration of 19 months from the priority date (Article 31).

5. ☒ A copy of the International Application as filed (35 U.S.C. 371(c)(2))

   a. ☒ is attached hereto (required only if not communicated by the International Bureau).

   b. ☐ has been communicated by the International Bureau.

   c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US).

6. ☐ An English language translation of the International Application as filed (35 U.S.C. 371(c)(2)).

   a. ☐ is attached hereto.

   b. ☐ has been previously submitted under 35 U.S.C. 154(d)(4).

7. ☐ Amendments to the claims of the International Aplication under PCT Article 19 (35 U.S.C. 371(c)(3))

   a. ☐ are attached hereto (required only if not communicated by the International Bureau).

   b. ☐ have been communicated by the International Bureau.

   c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.

   d. ☐ have not been made and will not be made.

8. ☐ An English language translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371 (c)(3)).

9. ☐ An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)).

10. ☐ An English lanugage translation of the annexes of the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)).

Items 11 to 20 below concern document(s) or information included:

11. ☐ An Information Disclosure Statement under 37 CFR 1.97 and 1.98.

12. ☐ An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.

13. ☒ A FIRST preliminary amendment.

14. ☐ A SECOND or SUBSEQUENT preliminary amendment.

15. ☐ A substitute specification.

16. ☐ A change of power of attorney and/or address letter.

17. ☐ A computer-readable form of the sequence listing in accordance with PCT Rule 13ter.2 and 35 U.S.C. 1.821 - 1.825.

18. ☐ A second copy of the published international application under 35 U.S.C. 154(d)(4).

19. ☐ A second copy of the English language translation of the international application under 35 U.S.C. 154(d)(4).

20. ☐ Other items or information:

U.S. APPLICATION NO (if known, see 37 CFR 1.5) 09/890846	INTERNATIONAL APPLICATION NO PCT/BY99/00011	ATTORNEY'S DOCKET NUMBER PAGA04US

21. ☒ The following fees are submitted:

CALCULATIONS PTO USE ONLY

BASIC NATIONAL FEE (37 CFR 1.492 (a) (1) - (5)):

Neither international preliminary examination fee (37 CFR 1.482)
nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO
and International Search Report not prepared by the EPO or JPO **$1000.00**

International preliminary examination fee (37 CFR 1.482) not paid to
USPTO but International Search Report prepared by the EPO or JPO **$860.00**

International preliminary examination fee (37 CFR 1.482) not paid to USPTO
but international search fee (37 CFR 1.445(a)(2)) paid to USPTO **$710.00**

International preliminary examination fee (37 CFR 1.482) paid to USPTO
but all claims did not satisfy provisions of PCT Article 33(1)-(4) **$690.00**

International preliminary examination fee (37 CFR 1.482) paid to USPTO
and all claims satisfied provisions of PCT Article 33(1)-(4) **$100.00**

ENTER APPROPRIATE BASIC FEE AMOUNT =	$ 860.00	
Surcharge of **$130.00** for furnishing the oath or declaration later than ☒ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492(e)).	$ 130.00	

CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE	$	
Total claims	56 - 20 =	36	x **$18.00**	$ 648.00	
Independent claims	4 - 3 =	1	x **$80.00**	$ 80.00	
MULTIPLE DEPENDENT CLAIM(S) (if applicable)			+ **$270.00**	$ 270.00	

TOTAL OF ABOVE CALCULATIONS =	$	
☒ Applicant claims small entity status. See 37 CFR 1.27. The fees indicated above are reduced by 1/2. +	$	
SUBTOTAL =	$	
Processing fee of **$130.00** for furnishing the English translation later than ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492(f)).	$ 0.00	
TOTAL NATIONAL FEE =	$ 994.00	
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). **$40.00** per property +	$	
TOTAL FEES ENCLOSED =	$ 994.00	
	Amount to be refunded:	$
	charged:	$

a. ☒ A check in the amount of $ ___994.00___ to cover the above fees is enclosed.

b. ☐ Please charge my Deposit Account No. _____ in the amount of $ _____ to cover the above fees.
A duplicate copy of this sheet is enclosed.

c. ☒ The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any
overpayment to Deposit Account No. 14-0783. A duplicate copy of this sheet is enclosed.

d. ☐ Fees are to be charged to a credit card. **WARNING:** Information on this form may become public. **Credit card
information should not be included on this form.** Provide credit card information and authorization on PTO-2038.

**NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR
1.137 (a) or (b)) must be filed and granted to restore the application to pending status.**

SEND ALL CORRESPONDENCE TO

DAVID NEWMAN CHARTERED
P. O. BOX 2728
LA PLATA, MARYLAND 20646

TELE. 301 934-6100

_____
SIGNATURE

DAVID B. NEWMAN
NAME

30966
REGISTRATION NUMBER

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of)
)
MISCHENKO, Valentin et al.)
)
Internat. App. No. PCT/BY99/00011)   Group Art Unit:
)
)   Examiner:
)
For: METHOD AND SYSTEM FOR)
AUTHENTICATION OF ARTICLES)
_____)

Honorable Commissioner of Patents
        and Trademarks
Washington, D.C.   20231

Sir:

PRELIMINARY AMENDMENT A

Prior to the initial Office Action, amend the application
as follows:

IN THE CLAIMS:

Amend the claims as follows:

8.   (Once Amended)   The method for marking articles
according to any of claims [1-7] 1-6, characterised in that

generating private keys, data encrypting and data
storing is effected in a remote control center;

applying the image, scanning the resulting image and
applying the encrypted code is performed by a marking means;

the marking means transmits data on the image to the
control center, while the control center transmits the
encryption result to the marking means; data transfer between

-1-

the marking means and the control center is effected through communication channels.

9.   (Once Amended)   The method for marking articles according to any of claims [1 -7] 1-6, characterised in that
generating private keys, data encrypting, generating a random image, applying the image on to the marked surface, reading the resulting image and applying the encrypted code on to the marked surface is performed by the marking means;
data transferring to the control center is also effected by the marking means, while at least keys are transferred to the control center through the path ensuring confidentiality;
the control center stores the keys and codes in the database.

12.   (Once Amended)   The method for identification, at an article checking terminal, of articles marked according to any of claims [1-11] 1-6, comprising
reading a marking image and transforming it into data
reading an encrypted code;
decrypting (recovery of the image data against the readout code);
comparing the recovered data with the readout image data
characterised in that
an additional criterion of existence of a respective texture on

the image is specified when identification, thereafter the image is readout.

15. (Once Amended) The method for identification of articles according to any of claims [12-14] 12, characterized in that errors are estimated in the process of comparing, and a decision is made on basis of a preset criterion.

REMARKS

By this Amendment, applicant amends claims 8, 9, 12, and 15. Claims 1-20 are pending in the application.

Replacement copies of claims 8, 9, 12 and 15 are attached herewith. Kindly enter this amendment prior to calculating the filing fee.

Respectfully submitted,

DAVID NEWMAN CHARTERED

By: _____
David B. Newman, Jr.
Date: _____August 6, 2001_____   Registration No. 30,966

T:\PAG-BY\PAGA04US_AM1.wpd

8. The method for marking articles according to any of claims 1-6, characterised in that

generating private keys, data encrypting and data storing is effected in a remote control center;

applying the image, scanning the resulting image and applying the encrypted code is performed by a marking means;

the marking means transmits data on the image to the control center, while the control center transmits the encryption result to the marking means; data transfer between the marking means and the control center is effected through communication channels.

9. The method for marking articles according to any of claims 1-6, characterised in that

generating private keys, data encrypting, generating a random image, applying the image on to the marked surface, reading the resulting image and applying the encrypted code on to the marked surface is performed by the marking means;

data transferring to the control center is also effected by the marking means, while at least keys are transferred to the control center through the path ensuring confidentiality;

the control center stores the keys and codes in the database.

12. The method for identification, at an article checking terminal, of articles marked according to any of claims 1-6,

-4-

comprising

reading a marking image and transforming it into data

reading an encrypted code;

decrypting (recovery of the image data against the readout code);

comparing the recovered data with the readout image data

characterised in that

an additional criterion of existence of a respective texture on the image is specified when identification, thereafter the image is readout.

15. The method for identification of articles according to any of claims 12, characterized in that errors are estimated in the process of comparing, and a decision is made on basis of a preset criterion.

METHOD AND SYSTEM FOR AUTHENTICATION OF ARTICLES

FIELD OF THE INVENTION

The present invention relates to the technique of protection of articles from counterfeiting, and may be used for protection from counterfeiting and unauthorized copying of goods. documents, securities, etc.

BACKGOUND OF THE INVENTION

A wide variety of methods for protection of documents and other goods from counterfeiting by means of marking them with special marks or labels are known in the prior art.

In some cases such marks are made of a special material having specific properties, e.g., a material that may be fluorescent in a particular light spectrum (US Patent 5,719,948 Apparatus and methods for fluorescent imaging and optical character reading), a material with magnetic features (US Patent 5,697,649 Articles employing a magnetic securities feature), or a material exhibiting anisotropy during absorption, reflection, transmission (US Patent 5,568,251 Authenticating system..), etc. Such materials may be also applied or included into a composition of a mark forming a particular figure. combination etc.

However, neither of the methods is able to provide total anti-counterfeit protection, since a pirate can recognize a material and use the same technique or even a higher one.

The other group of methods is based on the unique physical or chemical characteristics of a surface of a document or a product. For this purpose a section of the surface to be protected is scanned in accordance with the selected physical characteristic of a surface (WO97/24699 Authentication of articles). The scanned image is encoded and/or encrypted. and the obtained result is applied to the surface of an article or a document in the form of a numeral or a code. In the course of checking the authenticity, the surface is scanned by the testing device. The data obtained after scanning are processed by the same method, the code applied to the surface is decoded and/or is decrypted and compared to the result of processing of scanning.

Scanning of physical characteristics requires elaborated physical devices. The characteristics can have a wide pnysical range of variations and a high level of background characteristics. This fact makes their use rather expensive and reduces the degree of estimation validity. The major problem consists in determining the area of scanning, since use of the physical characteristics of a surface does not limit the scanning area to the proper physical characteristics impeding possibility of re-getting to the same region. Moreover. the encoding systems now in use, fail to provide a sufficient crypto-resistance of encoding, and the used keys may be restored for counterfeiting.

Specially structured materials, comprising randomly distributed fibers or other contrast inclusions that are easily readout by optical devices set for transmission or reflection (WO98/57299 Document with an authentication feature), are used for more reliable determination of random characteristics of a surface. In this case the scanning
5   area is limited to special patterns or windows, that are applied to the surface of a label made of a structured material.

The labels of the kind may be manufactured and tagged to articles or documents. However, during re-readout the bulk structure and optical characteristics of fibers may cause errors leading to uncertainty of identification, on the account of errors in
10   determining scanning areas, as well as because of inaccuracy in measuring medium characteristics. Moreover, such identification system requires elaborated equipment for precise determining of spatial optical characteristics. The similar system uses a label with randomly (irregularly) disposed dichroic fibers. Information on the producer, characteristics of the goods and information on the encoded result of scanning is
15   disposed next on a label (WO99/17486 System and method for authentication of goods). However, the system requires special reading equipment for determining the optical characteristic of dichroity of fibers. In addition, disposition of fibers in the medium and inaccuracy in determining binding of fibers may result in considerable inaccuracies during re-readout while testing.

20   Additionally, during analysis of a great number of tags, the encoding system may also be "opened", and tags may be counterfeited or simply transferred from original goods to counterfeited articles.

Prior art also discloses methods of protection of documents from copying by means of applying nonreplicable pitches to an image, e.g. press printed lineatures, etc.
25   (US Patents: 5,018,767 Counterfeited protected document; 5,193,853 Nonreplicable document and method for making same).

However, the said methods do not allow to identify quickly the article that may be counterfeit.

Methods and systems for protection of documents and postal matters from
30   counterfeiting are also disclosed in the prior art. (US 5,970,151 Method and arrangement for generating and checking a security impression) In accordance with the patent, specially encoded images and digits are applied to a document or to an envelope; the data on the said images and digits are stored in a remote control center. During checking a document image is scanned, encoded and transmitted to the data storage center, the
35   data are compared to the stored value. Thereafter a conclusion on authenticity of a document is drawn.

The printed contrast image facilitates readout and increases reliability of identification of marking. Moreover, such methods provide a rather reliable control of document passage. However, the marking of the kind may be copied and applied onto another document, i.e. it may be counterfeited by substituting a document.

5   The prior art authentication systems generally comprise at least two remote scanners, a printing device, data processing means and communication means.

In the prior art systems a printing device imprints information and a code. Moreover, in the system under the US patent 5,970,151 the printing device imprints an encoded image, as well as a sequence of bar codes or terminal codes.

10   The described systems require the elaborated scanning equipment and special composite mediums (materials) for reliable re-scanning under testing. On the other hand, increase of image contrast and reproducibility of repeated scanning in existing systems magnifies probability for copying and counterfeiting.

The closest technical solution for the system under the present invention is the
15   system and method of marking goods disclosed in the US patent 5,592,561. The said system comprises a control computer, a main computer, a marking system and a testing reader, all of the devices being compatible and connected by a communication system. The marking system comprises a printer, a reader, and a processing and control unit that is connected to the main computer by a modem. Marks in the form of a two-dimensional
20   encrypted image are imprinted on an article or on a material the product is made of.

The image may be scanned by a reading device and encrypted in the form of encrypted data. Then the data are compared with the authentication data of the database, or the data are decoded and compared with the data stored in the central database of the main computer.

25   The marking system ensures control of image printing by means of a certain number of authentication codes, which should be applied prior to that, when the re-authentication is required. When printed, the encoded image is scanned and recognized as a true one in the central database. Then the image may be stored in the database together with the relevant information referring to the said particular product.

30   During checking goods, alongside with authentication the goods are tested in respect of duplication of unique codes, whereby counterfeited goods are so detected.

The system provides a fairly sharp and easily readout image. Nevertheless, the system is not able to defend the producer from counterfeiting in a full scope, since an image is easily reproduced, and a counterfeited copy of a product may happen to be the
35   first one during re-testing of mass goods.

The aim of the invention is development of a reliable method and system for recognizing of marking, uniqueness of marking, as well as control of movement of goods.

4

SUMMARY OF THE INVENTION

The present invention develops new methods for marking articles and authentication the same, as well as a system for checking and authenticating, i.e. checking the genuiness of origin of goods, articles and documents.

5   The main aim of the invention is providing a marking means that is, on one hand, capable of ensuring a unique marking and impossibility for counterfeiting of the marking, and, on the other hand, is satisfactory secure and simple in technicality of recognizing unique marking.

The aim of the invention is realized in the following way. Marking of articles is performed

10   by the steps of:

- generating private keys;

- storing the said keys in the database;

- generating an image for each sample of an article;

- applying the image on the marked surface;

15   - reading the resulting image;

- obtaining data on the read-out image;

- encrypting the said obtained data;

- applying the resulting code onto the marked surface.

The method is also characterized by that a unique image is generated as a random at

20   least two-dimensional image; and the said generated random two-dimensional image is applied on to a selected area, made of a material that has a rough surface with random characteristics;

Various materials may be used, e.g. materials having a rough surface, fibrous, porous material, materials with inclusions of particles, etc.

25   In this case the cheapest materials are fibrous materials, including rough paper, cloths and other household materials. The said materials ensure impossibility of any copying, whereas a completely another image is produced, under re-applying any image on a surface of a random texture. This is due to the fact that, in the process of dyeing, a distribution of coloring or any other marking agent is essentially influenced by the texture.

30   On the other hand, the intensity of reflected light also substantially influences image characteristics during reading. Thus, the image of this kind may produce a completely different identification data when readout. In this case the counterfeited article will be immediately identified. Accordingly, marking of this type provides both the unique character of marking and impossibility for any replication by modern technical means,

35   providing also the unique character of the identification code applied next to the marking image.

5

Further improvement of the invention is performed according to the following distribution of functions for the constituent parts of the system:

- generating private keys, data encrypting and data storing is effected in a remote control center;

5
- applying the image, scanning the resulting image, and applying the encrypted code is performed by a marking means;

- data exchange between the marking means and the control center is effected over communication channels;

10 The abovementioned distribution of functions provides protection from counterfeiting by safe storing the encryption keys, which are designed for creating protection codes applied onto a label next to the identification image. The individuality of keys prevents possibility of encrypting any other randomly generated counterfeiting images.

15 According to another embodiment of the invention a producer or a supplier may take up the running of protecting marking. In this case the functions may be distributed as follows:

- generating private keys, data encrypting, generating a random image, applying the image on to the marked surface, reading the resulting image and applying the encrypted code on to the marked surface is performed by the marking means;

20
- data transferring to the control center is also effected by the marking means, while at least keys are transferred to the control center over the path providing confidentiality;

- the control center stores the keys and codes in the database.

In this case the control center provides only the monitoring and checking function.

25 The other method for obtaining a unique marking image that frames conditions for impossibility of reproducing and counterfeiting, is a variant of embodiment, according to which, using the same actions and data processing sequence, a random image is applied onto a surface, that is further modified for forming a texture with random parameters. In this case, a random two-dimensional image is applied to the surface, which is further

30 modified, gaining as a result the similar anti-counterfeiting features as in the previous case. Preferably, the surface therewith is modified until a steady texture with random parameters is formed.

The aforementioned surface modification may be effected by any of the beneath disclosed methods or by equivalent techniques, e.g. by perforating. In this case, the

35 texture and its random parameters are formed at the edge of openings on account of both - erosion of the edge and it's matching with random image elements and their parts.

6

Perforating may be also performed by electrospark machining. In this case distribution of openings is also random and nonreproducible.

The surface may be also modified by texture impression, by analogy with seals, pressing means, etc.

5   Further means for image modifying and providing nonreproducibility may be the use of a porous material with capillary features. In this case, porosity defines a texture existence, while the image is modified in a random way on the account of irregular re-distribution of a liquid colorant throughout irregular layout of capillaries.

The articles marked in accordance with the present invention are identified in the
10   checking terminal. In this case, the following prior art operations are fulfilled:

- reading a marking image;

- reading an encrypted code;

- decrypting the encrypted code for data recovering;

- comparing the recovered data with the readout image data.

15   Unlike the prior art authentication methods, according to the present invention the criterion of existence of a respective texture on an image is specified, when identifying, thereafter the image is readout. In accordance with one embodiment, functions between the checking terminal and the control center are distributed as follows:

- specifying the feature of texture existence, reading the marking image and reading
20   the encrypted code is effected in the checking terminal; the readout image data
       being transferred to the control center;

- decrypting (recovery of the image data against the readout code), comparing the
       recovered image with the data of the readout image is effected in the remote
       control center.

25   According to another embodiment

- reading the marking image, reading the encrypted code and specifying the
       criterion of texture existence is effected at the checking terminal; the readout
       image data being transferred to the control center;

- decrypting (recovery of the image data against the read-out code) is effected in
30   the remote center, and the recovered result is transferred to the checking terminal;

- comparing the recovered data with the readout identification image data is
       effected in the checking terminal.

In the described authentication systems, the additional criterion, i.e. existence of a texture on a surface, is the decisive criterion for starting the identification process.
35   The said criterion closes out marking imitation of by means of exact reproducing of a flat sample (copy) of the original marking. Texture existence conditions impossibility of

7

any counterfeiting, as in the process of applying an image on to the texture surface the resulting image changes in a random way, and cannot correspond to the original image.

5   Actually, during image readout, some deviations may occur between the first and the second readout. The deviations are conditioned by both - the endurance of the label and by the characteristics of the reader. The deviation limits may be preset as they are established in accordance with practice or tests. Therefore, modern identification methods generally compare characteristics of the obtained images, but not of the
10   obtained codes. In the process of comparing errors are estimated. Decisions are made on basis of the pre-set criterion.

In general, in accordance with the present invention, the whole process of identification of articles, starting from marking to making decision on authenticity of an article, together with testing passing of products and search for counterfeiting products,
15   comprises the following steps:

- pre-marking of articles;

- reading the resulting image;

- data encrypting;

- data storing in the control center database;

20   - re-reading (checking) the unique image;

- data transfer to the control center;

- data comparing with the data stored in the database;

The said method differs from the prior art methods by that a marking image is obtained by the following steps:

25   - generating a random unique image as at least a two-dimensional image;

- applying the generated random image to a surface having a roughness with random parameters,

- reading the resulting image;

- transferring data on the read-out image to the remote control center;

30   - generating private keys;

- encoding the obtained unique image data by means of private keys;

- transferring the resulting code to the marking station and applying the code onto the marking surface;

- storing the keys in the control center database;

- verifying the existence and the pattern of the texture on the marking surface in the checking terminal; and then
- test reading of the marking image and the applied code;
- transferring the data on the code to the control center;
- decrypting the data on the code and recovering the data on the readout image;
- transferring the recovered data to the checking terminal for comparing them with the data on the readout image, and making decision on the authenticity of the article.

The said embodiment of the invention is preferable, as it reduces the traffic value for communication network. At the same time, while comparing image data at the checking terminal, i.e. at the unit of storing direct information on the checked article and its state, one may estimate the situation more objectively. In addition, when considerable deviations in quantitative characteristics are registered, it is possible to check some other articles from the series.

On the other hand, image data may be also transferred to the control center for comparing the data obtained at check scanning with the data, recovered against the obtained code.

The said method is characterized by that a unique marking image is obtained by the steps of.

- generating a unique image as a random at least two-dimensional image;
- applying the generated random image to a surface having a texture with irregular parameters;
- reading the resulting image;
- transferring data on the read-out image to the remote control center;
- generating private keys;
- encrypting the obtained unique image data by means of private keys;
- applying the resulting code on to the marking surface;
- storing the keys and the unique image data in the control center database;
- verifying the existence and the pattern of the texture on the marking surface in the checking terminal; and then
- test reading of the marking image and the applied code;
- transferring the readout data to the control center;
- decrypting the data on the code and recovering the data on the read-out image;
- comparing the recovered data with the image data received after the test reading;

•   transferring the results of comparing to the checking terminal.

Further improvement of the method for identification of articles and monitoring of product passing with a view of determining counterfeited articles and timely preventing of infringement is characterized by that the control center stores data on the checks performed, a number of checks of one and the same code being registered, when the set value of checks being exceeded, a signal informing on the recurring request is produced.

For technical implementation of the aforementioned methods, there may be created systems for identification of goods, consisting in an equipment complex, and their structure comprising:

•   a marking station,

•   an control center,

•   checking terminals;

•   communication means;

•   data transfer media.

The system for authentication of articles comprises a marking means including a printer, a printer control device, a readout device, an image processing unit, a communication means and a remote control center and a checking terminal comprising a key generating unit, encoding/decoding unit, a memory unit, a compare facility (decision-making unit), and blank parts for labels. In accordance with the present invention the marking device further includes a random image generating device, means for applying an encrypted code; as blank parts for labels are used substrates made of material having a texture with random parameters.

In general, implementation of the proposed method results in a new positive effect, which is characterized by the following.

On the one hand, reliability of multiple readout is magnified due to generating and applying on the identified surface of the image having the characteristics that are optimal for qualitative multiple readout.

In this case the scanning area of the protective image is precisely localized, since the applied image has a good contrast in comparison with the remaining surface.

On the other hand, storing of the private keys in remote processing center magnifies the degree of reliability for storing private keys, which are never transmitted to open checking terminals, and in general, may be transmitted nowhere at all.

In addition, use of a texture substrate or any other random three-dimensional image transforming, practically excludes any possibility for simple copying of labels. In

this case the structure of the surface by itself serves as an additional criterion for pre-identification (visual identification).

In accordance with the present invention some more advantages may be achieved by further development thereof.

5   Additional testing of labels in the view of replication-prevention still further boosts the degree of anti-replication protection, providing thereby effective detection of counterfeiting cases. Thus, for example, if the infringer "selected" a possibility for reproducing or otherwise counterfeiting the labels in one or several variants, then frequent appearing of identical labels may be detected and localized.

10   DESCRIPTION OF DRAWINGS

Fig. 1 shows a label containing an applied image and a bar code;

Fig. 2 shows a general scheme of the system for authentication of articles or documents;

Fig. 3 shows a block scheme of the marking station,

Fig. 4 shows a block scheme of the checking terminal,

15   Fig. 5 shows a block scheme of the control center,

The method and the system according to the invention will be better understood by an example of a label shown in Fig.1

A label is a card attached to an article or a document and may be coupled to it in a one-piece fashion.

20   A label may contain general information 2, i.e. a trademark, kind of an article, its parameters etc. Additionally, a label may also comprise an identifying image 3 and its encrypted image in the form of a bar code 4. The said bar code may also contain some other service information about keys, a serial number, etc. The surface in the area of the identification image may be covered by a special material providing roughness of the said

25   surface.

In general, the identification system, as shown in Fig. 2, may be delivered in a computer variant with of special or universal processors. In this case the system comprises a marking device, which includes at least a printer 5, a scanner 6 and a marking processor 7 that functions for random image generating, for data processing and

30   printer control, and a means for data transmitting 8 over a distributed or local network 9. The control center comprises a central processing unit 10 and at least a memory device 11 for storing of databases, and an encoding/decoding unit 12. Over communication means 8 the said center is also inline (online) to the worldwide or local data transmitting network 9.

The said center is further connected to the remote checking devices, each of them comprising at least a communications means 8, a scanner 6 and a data processor for checking 13.

The system may also comprise a set of blank parts for labels.

5   In accordance with the invention an image (picture) is generated by the image generator 14 in the marking station, as shown in Fig. 3. The image comprises dots, randomly "scattered" within the limits of the set area of dots (pixels), or fully consists of the said dots; each dot is assigned its own color, which is randomly sampled every time from an n-color palette.

10   The generated image is imprinted on to a surface of a label with the help of a jet or laser printer 5 having a 300 dpi resolution.

The substrate 15 for a label is made of a material with a relief surface, such as friable paper, fabric or porous material. The obtained image may be randomly transformed by means of a special device in the process of printing or after the same.

15   The surface texture of these materials is distributed in a random way. Therefore, unlike a generated image, dyes or printer toner filling surface irregularities is re-distributed. Additionally, in the process of further readout reflection characteristics vary according to texture inclination.

The image has still one more advantage. In the process of replication to a similar surface, toner particles arrive in other conditions, and, accordingly, the image varies

20   again, and cannot be copied in facsimile on a similar surface because of mismatch of a random surface texture with the image element of the original.

The imprinted image may also be transformed in another way, e.g. by perforating, expansion or compression, heat treatment, etc.

25   In these cases important is the spatial structure of a substrate, since a structure is the main bar for prevention from identical copying, serving thereby as an additional authentication criterion.

When the said image is imprinted, the area is scanned by the scanner 16 of a 300dpi resolution. 256 shades of gray.

30   As a result of scanning, a raster array of an 8bpp color depth is obtained.

The resulting array is processed in DIB (device independent bitmap)- processo16 according to the preset rule, e.g. by interleaving to fractions according to colors. Pixels of some fractions are excluded from the total number of the array pixels. The number N_1 of the other pixels is defined together with their average color intensity

35
$$N_2 = (C_1 + C_2 + \ldots C_{N1})/N_1$$

12

The line of symbols obtained by concatenation of line expressions of hexadecimal representation of N_1 and N_2, is the image representation. The said line of symbols is encrypted by a private key, e.g. as disclosed in PCT/99BY/00004 (MZ4).

A private key may be either generated in the marking station or transmitted to control center, or it may be obtained from the control center, shown in the Fig. 4. In this case, an individual private key is generated by the key generator 19 for every marking terminal. To provide higher security, in particular, for marking individual objects, an image representation may be sent for encrypting to the control center. Then, the obtained encrypted image representation is transmitted from the control center to the marking station. As shown in Fig 1, the bar code generator 17 transforms the encrypted image representation into a bar code, which is imprinted by printer 18 to the label surface next to the image as a bar code 3.

As shown in Fig. 4 the control center includes input/output communication units (modem) 8, a code generator 19, an encoder/decoder 20, a compare facility 22 (that may be also located at the checking terminal), a memory device 23 for storing data on the carried out tests, etc.

When data on the testing image arrive from the marking terminal at the input of the control center, the key generator 19 generates a private key, which is stored in the database 21. Then the private key is transferred to the encoder/decoder 20, where the image representation is coded and transferred back to the marking station for imprinting to a label as a bar code 3.

If the code data arrive at the input of the control center from the checking terminal, the encoder/decoder 20 requests the database for a key in accordance with ID of the bar code. The respective key arrives at the decoder 20, which recovers (decodes) the image data. Thereafter, the said data are transferred through the compare facility 22 to the decision-making unit 25 of the checking terminal, as shown in the Fig. 5.

Testing data are stored in the database 23. In case some bar codes occur often, the unit 22 blocks transmission of the recovered image representation and issues a counterfeit signal.

As shown in Fig. 5, the checking terminal is equipped with a bar code reader 24, an image scanner 6, a DIB (device independent bitmap) processor 16 for image identification, an input/output unit of the communication channel 8, and a compare and decision-making device 25. In the checking terminal the protective image 2 is scanned, and the protective bar code 3 is readout.

The value of a bar code 3 of the encrypted image representation is readout and sent over a communication channel 9 to the control center.

13

The control center selects the relevant key from the memory device 21 of the key database, decodes the set value, recovering thereby the image representation expressed by the N_1 'and N_2 ' parameters.

The recovered image representation is transferred back to the checking terminal. The comparing and decision-making device 25 compares the said image with the image representation obtained as a result of check scanning by the scanner 6 of the imprinted image and processing in the DIB processor 16 by the N1 and N2 parameters. The result of comparing of the N_1' and N_2' parameters with the N_1 and N_2 parameters is analyzed for making decision on authenticity or counterfeit of an article. In the process are estimated permissible deviations of parameters values caused by wearout of a label, inaccuracy of scanning, etc.

A marking station may be located either at an enterprise-producer or at a centralized storage, or in special station for certifying documents, e.g. notary's office, etc.

The identification station should be reasonably secure to ensure protection of the stored information, keys and testing data and other information.

The checking terminal may be arranged as accessible to public terminals, such as bancomats. located in large shopping centers or other public facilities.

In accordance with the invention, the Internet, telephone, designated local or other networks may be used for communication. Protected communication channels are preferable.

Thus, under the proposed method and the system based on it, authentication of articles and/or documents is performed with use of standard technical means, At the same time counterfeit-protection is ensured on the account of unique images, imprinted on a carrier with random three-dimensional structure. This combination, together with use of a system of remote secure control center with theoretically crypto-resistant private keys, provides a reliable counterfeit-protection.

Finally, the system provides counterfeit-protection of goods and documents without using any complex and specific physical protection means. This fact makes the system obtainable, moderate and cheap.

From the foregoing it will be understood that the invention provides a highly effective method and system for counterfeit-protection of articles and documents. While the invention has been described in its presently preferred form, it will be understood that the invention is capable of modification without departing from the spirit of invention as set forth in the attached claims.

CLAIMS

1. A method for marking articles, comprising

- generating private keys;

- storing the said keys in the database;

5   • generating an image for each sample of an article;

- applying the image on to the marked surface;

- reading the resulting image;

- obtaining data on the readout image;

- encrypting;

10   *characterized in that*

- an image is generated per each sample of an article, as a unique and random at least two-dimensional image;

- the said generated random two-dimensional image is applied on to a selected area made of material having a roughness surface with random parameters;

15   • the data on the readout image are encrypted; and

- the resulting code is applied on to the marking surface.

2. A method for marking articles, comprising

- generating private keys;

20   • storing the said keys in the database;

- generating a image for each sample of an article;

- applying the image on to the marked surface;

- reading the resulting image;

- obtaining data on the readout image;

25   • encrypting;

characterized in that

- a image is generated per each sample of an article, as a unique and random at least two-dimensional image;

- the said generated random two-dimensional image is applied on to a selected

30   surface area; and thereafter

- the surface with the applied image is modified until a irregular three-dimensional texture is formed;

- the resulting image is readout after the surface is modified; and thereafter

- the data on the readout image are encrypted; and

- the resulting code is applied on to the marking surface.

3. The method for marking according to claim 2, characterized in that the surface is modified until a steady texture of random parameters is formed.

4. The method for marking according to claim 2, characterized in that the surface is modified by perforation.

5. The method for marking according to claim 2, characterized in that the surface is modified by embossing.

6. The method for marking according to claim 2, characterized in that the surface is modified by electrospark machining.

7. The method for marking according to claims 1 or 2, characterized in that as a marking material is used a label with a selected area of a three-dimensionally patterned material, such as a porous material having capillary features.

8. The method for marking articles according to any of claims 1-7, *characterised in that*

- generating private keys, data encrypting and data storing is effected in a remote control center;

- applying the image, scanning the resulting image and applying the encrypted code is performed by a marking means;

- the marking means transmits data on the image to the control center, while the control center transmits the encryption result to the marking means; data transfer between the marking means and the control center is effected through communication channels;

9. The method for marking articles according to any of claims 1 -7, *characterised in that*

- generating private keys, data encrypting, generating a random image, applying the image on to the marked surface, reading the resulting image and applying the encrypted code on to the marked surface is performed by the marking means;

- data transferring to the control center is also effected by the marking means, while at least keys are transferred to the control center through the path ensuring confidentiality;

- the control center stores the keys and codes in the database.

10. The method for marking articles according to claim 2-6, characterized in that

- generating private keys; data encrypting and storing is effected in the remote control center;

- applying the image, modifying the surface texture with the applied image, scanning the resulting image and applying the code is performed by the marking device;

- data exchange between the marking means and the control center is performed over communication channels.

11. The method for marking articles according to claim 1, characterized in that

- generating private keys; data encrypting, as well as applying the image, scanning the resulting image and applying the code is performed by the marking device;

- the marking means transmits the data on the image to the control center, which stores them in the database; at least the keys are transferred to the control center by the path ensuring confidential transmission.

12. The method for identification, at an article checking terminal, of articles marked according to any of claims 1 -11, comprising

- reading a marking image and transforming it into data

- reading an encrypted code;

- decrypting (recovery of the image data against the readout code);

- comparing the recovered data with the readout image data

characterised in that

- an additional criterion of existence of a respective texture on the image is specified when identification, thereafter the image is readout.

13. The method for identification according to claim 12, characterized in that

- reading the marking image, reading the encrypted code and specifying the criterion of texture existence is effected at the checking terminal; the readout image data and the readout encrypted code are transferred to the control center.

- decrypting (recovery of the image data against the read-out code), comparing the recovered image with the data of the readout image is effected in the remote control center.

14. The method for identification according to claim 12, characterized in that

- reading the marking image, reading the encrypted code and specifying the criterion of texture existence is effected at the checking terminal; the readout code data being transferred to the control center.

- decrypting (recovery of the image data against the read-out code) is effected in the remote center, and the recovered checking result is transmitted to the checking terminal;

- comparing the recovered data with the data of the readout identification image is effected in the checking terminal.

15. The method for identification of articles according to any of claims 12-14, characterized in that errors are estimated in the process of comparing, and a decision is made on basis of a preset criterion.

16. A method for authentication and detection of counterfeited articles comprising the steps of:

- pre-marking of articles by applying a unique two-dimensional image on to the marking space;

- reading the resulting image, transferring data on the image to the remote control center;

- data encrypting;

- data storing in database;

- re-reading the unique image at least in one of the remote checking terminals;

- data transfer to the control center,

characterized in that a unique marking image is obtained by the following steps:

- generating a unique image as a random at least two-dimensional image;

- applying the generated random image to a surface having a texture with irregular parameters;

- reading the resulting image;

- transferring data on the readout image to the remote control center;

- generating private keys;

- encrypting the obtained unique image data by means of private keys;

5   - transferring the resulting code to the marking station;

- applying the resulting code on to the marking surface;

- storing the keys in the control center database;

- verifying the existence and the pattern of the texture on the marking surface in the checking terminal; and then

10   - test reading of the marking image and the applied code;

- transferring the code data to the control center;

- decrypting the code data on the and recovering the data on the readout image;

- transferring the recovered data to the checking terminal;

- comparing the recovered data with the data on the readout image;

15   - making decision on the authenticity of the article.

17. A method for authentication and detection of counterfeited articles comprising the steps of:

- pre-marking of articles by applying a unique two-dimensional image on to the
20   marking space;

- reading the resulting image, transferring the image data to the remote control center;

- data encrypting;

- storing data in the control center database;

25   - re-reading the unique image at least in one of the remote checking terminals;

- data transfer to the control center;

- data comparing with the data stored in the database;

- transferring the result of comparing to the checking terminal;

characterized in that a unique marking image is obtained by the steps of:

30   - generating a unique image as a random at least two-dimensional image;

- applying the generated random image to a surface having a texture with irregular parameters,

- reading the resulting image;

- transferring data on the readout image to the remote control center;
- generating private keys;
- encoding the obtained unique image data by means of private keys;
- transferring the encoded image to the marking station;
5
- applying the resulting code on to the marking surface;
- storing the keys in the control center database;
- verifying the existence and the pattern of the texture on the marking surface; and then
- test reading the marking image and the applied code;
10
- transferring the readout image data and the code to the control center;
- decrypting the code data and recovering the readout image data;
- comparing the recovered data on the image received after the check reading;
- transferring the results of comparing to the checking terminal.

15   18. The method for authentication according to claims 16, 17, characterized in that the data on the performed tests are stored in the control center; the number of the same code tests being summarized, and when the set value is exceeded, a signal warning on the exceedence is produced.

20   19. The system for authentication of articles according to claim 1, comprising a marking means including
- a printer,
- a printer control device,
- a readout device,
25
- an image processing unit,
- a communication means; and
- a remote processing and storage center, comprising,
- a key generating unit,
- an encrypting/decrypting unit,
30
- a memory unit,
- a compare facility, and

blank parts for labels,

characterized in that the marking device further includes

- a random image generating device,

- means for applying an encrypted code; and

- as blank parts for labels are used substrates made of material having a texture with random parameters.

5

20. The system for authentication of articles according to claim 2, comprising a marking means including

- a printer,

- a printer control device,

10
- a readout device,

- an image processing unit,

- a communication means; and

- a remote processing and storage center, comprising,

- a key generating unit,

15
- an encrypting/decrypting unit,

- a memory unit,

- a compare facility, and

blank parts for labels,

characterized in that the marking device further includes

20
- a random image generating device,

- means for applying an encrypted code; and

- means for transforming surfaces of labels into three-dimensional texture with random parameters.

1/5

2

1

4

3

Trade mark

PRODUCT: Shoes for men

MODEL: 001-39437846767

SERIAL No: 123288005

BATCH: 200014

MADE ON: 22/09/1999

ATTENTION!
You can test this label in any
place where the check terminal
is installed .

23288005

Fig. 1

Fig. 2

MARKING STATION

Fig.3

CONTROL CENTER

Fig. 4

09/890846

5/5

CHECKING TERMINAL
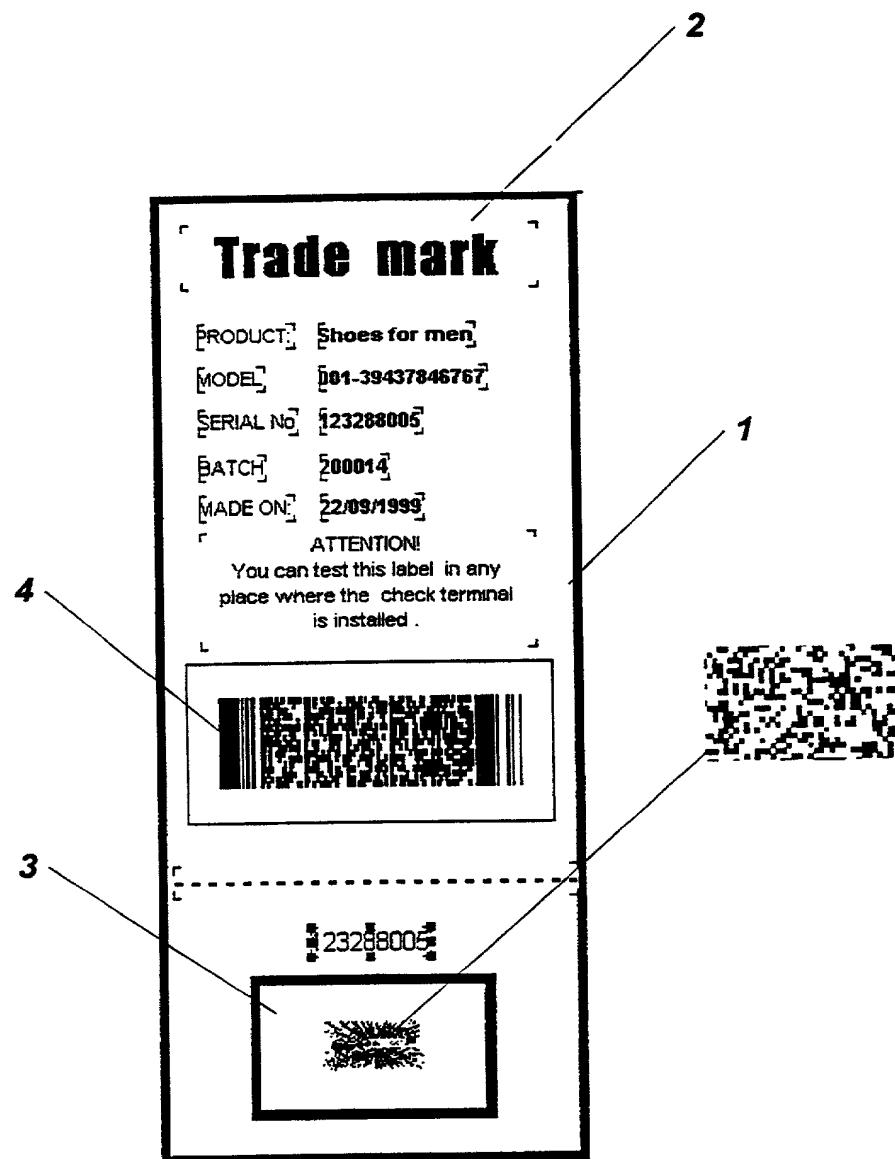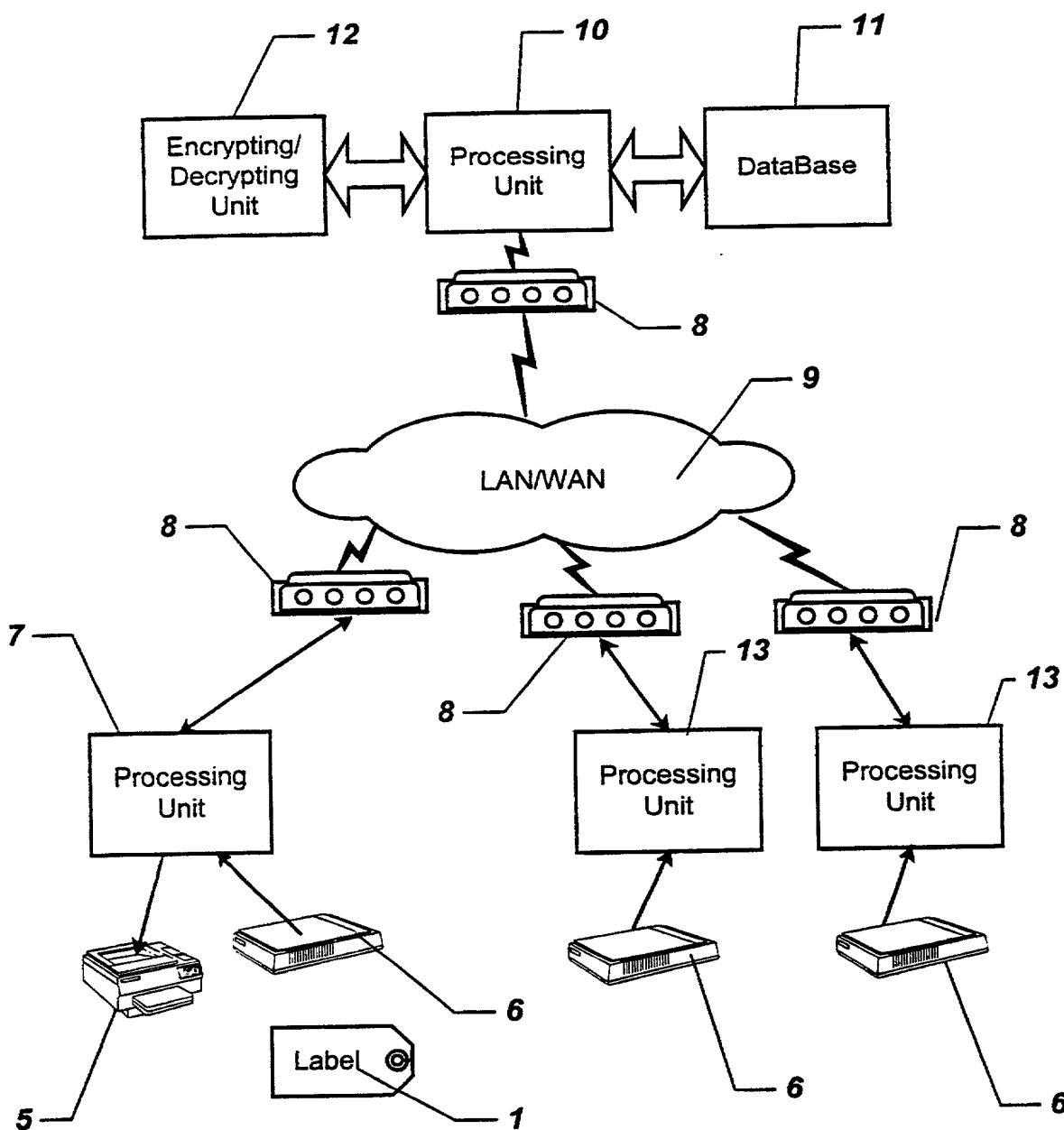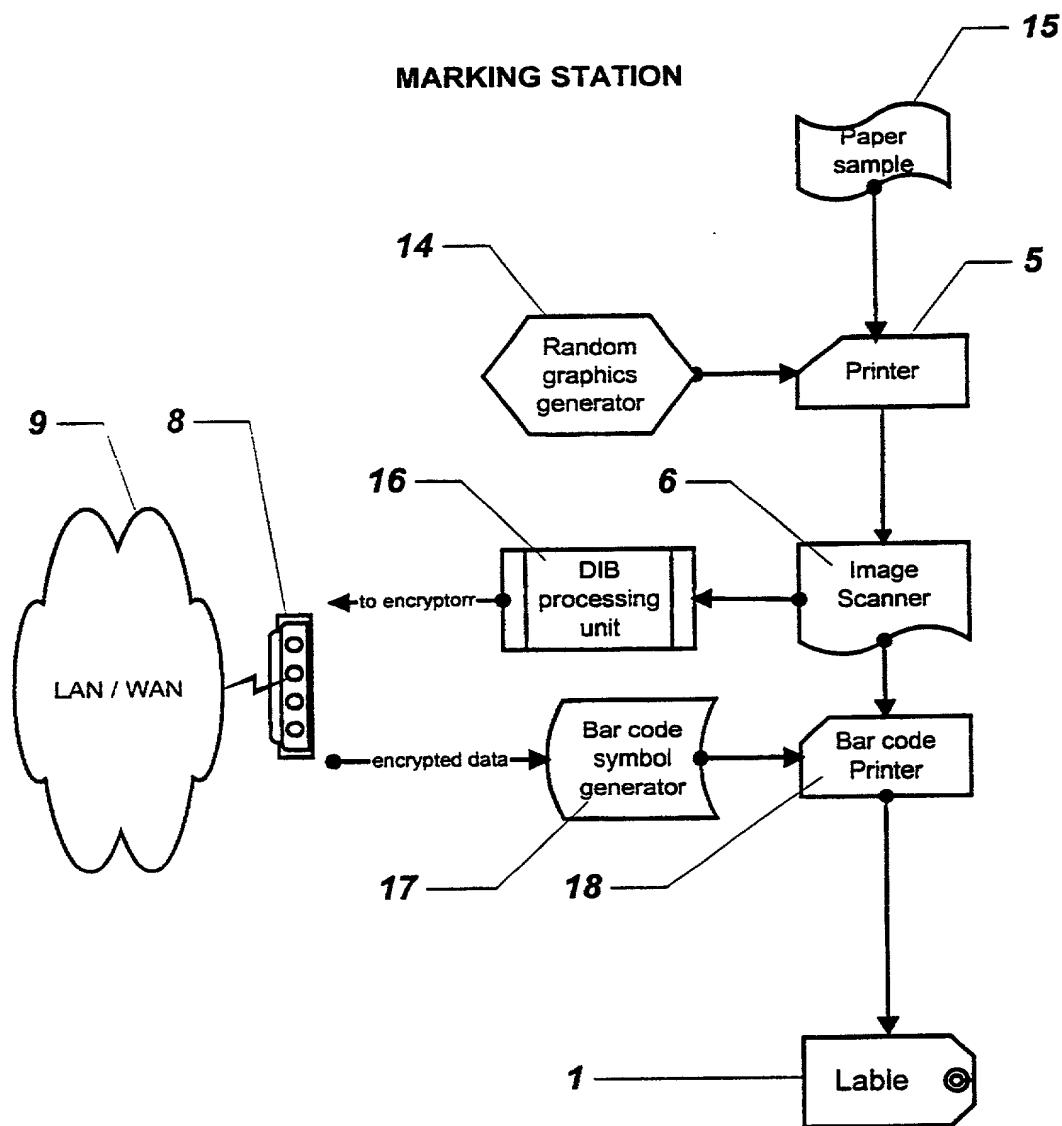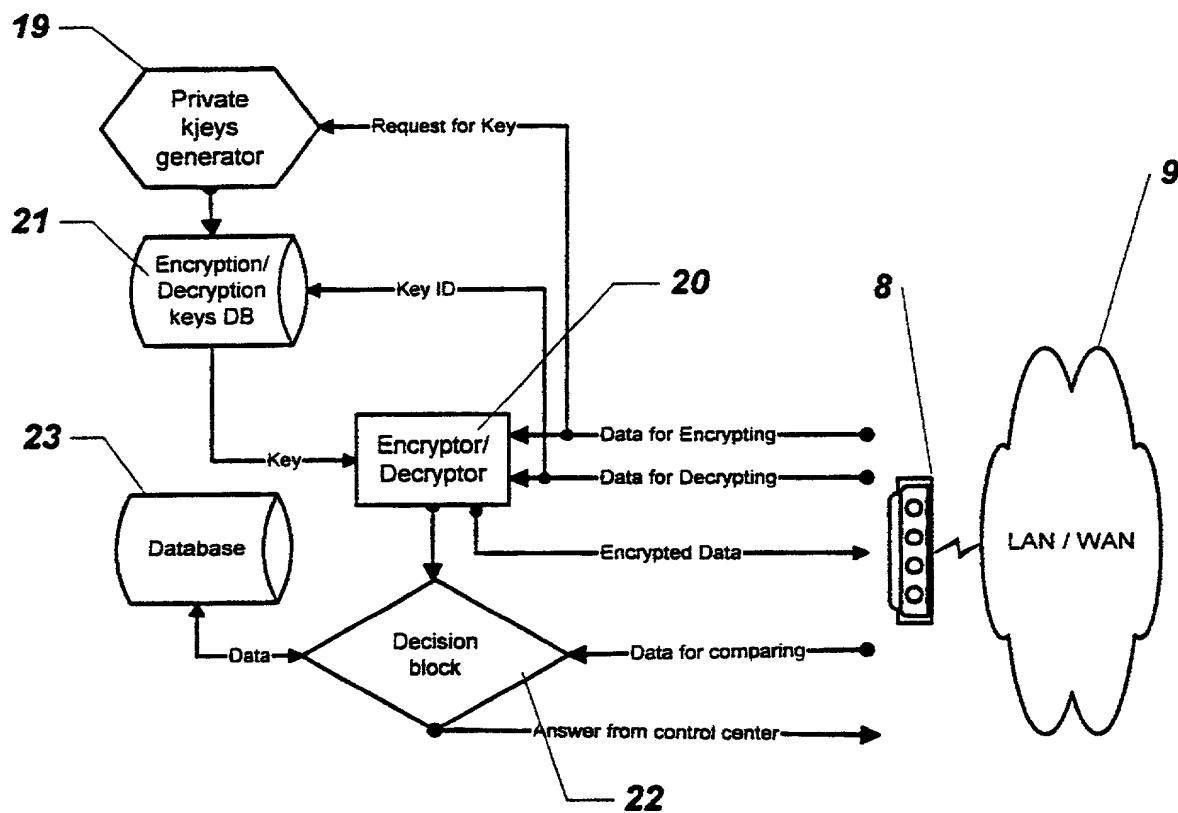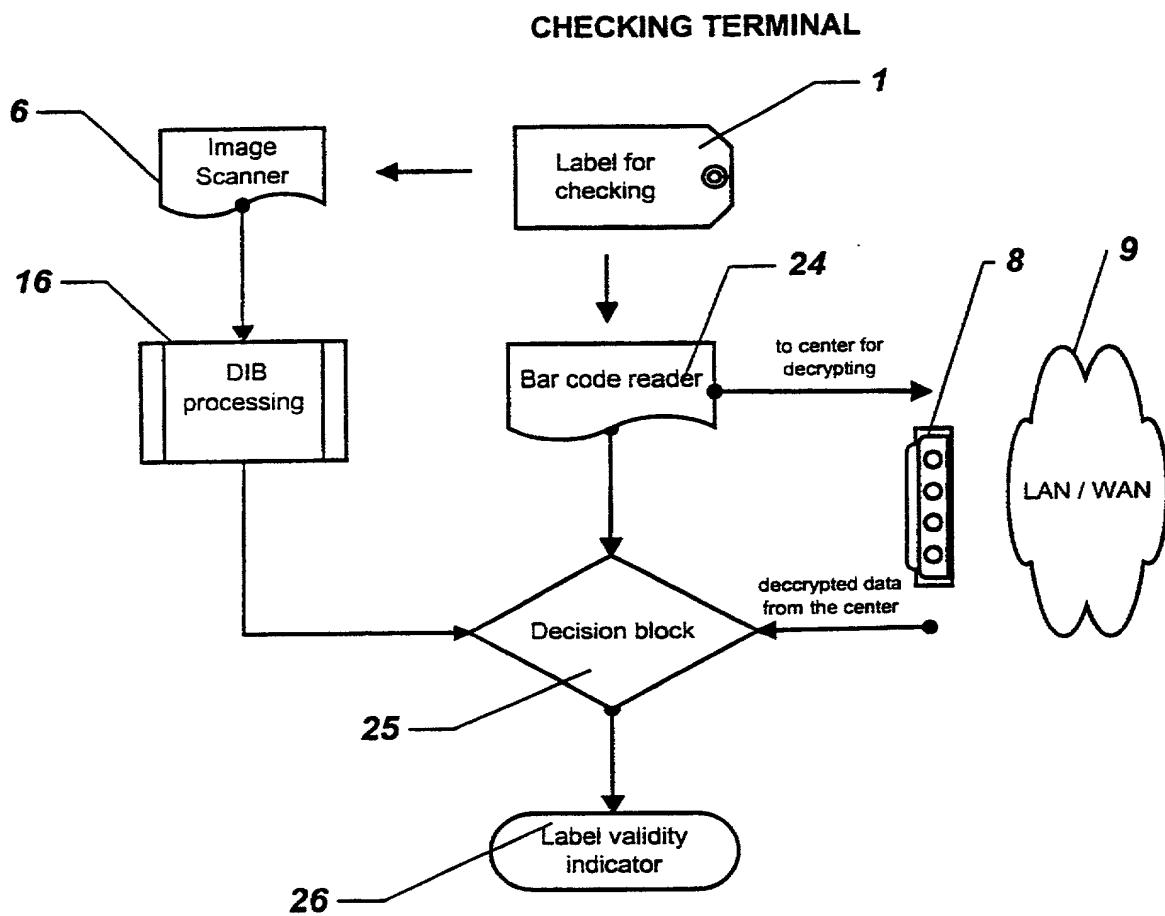
Fig. 5

Declaration and Power of Attorney for Patent Application

Заявление о подаче заявки на патент и доверенность поверенному

Заявление на русском языке

Russian Language Declaration

Я, нижеупомянутый изобретатель, настоящим подтверждаю, что:

Мое местожительство, почтовый адрес и гражданство действительно таковы, как указано ниже, непосредственно после моего имени.

Я убежден, что я являюсь первоначальным, первым и единственным изобретателем (если ниже указано только одно имя), или одним из первоначальных и первых со-авторов (если ниже указаны несколько имен) заявляемого изобретения, на которое запрашивается патент и которое называется:
СПОСОБ МАРКИРОВКИ И ИДЕНТИФИКАЦИИ ИЗДЕЛИЙ

Описание изобретения приложено к сему (если в расположенной ниже клетке нет отметки):

09/890,846

☐ было подано /дата/_____
как заявка США номер или международный PCT №
_____ с изменениями, внесенными /дата/
_____ (если требуется).

Настоящим я заявляю, что я изучил и понимаю содержание вышеназванного описания, включая формулу изобретения со всеми поправками, указанными выше.

Я признаю обязанность сообщить информацию, необходимую для патентования в соответствии с §1.56 раздела 37 Кодекса Федеральных Правил.

Настоящим я предъявляю иностранные преимущественные права приоритета в соответствии с §119 (a)-(d) или §365 (b) раздела 35 Кодекса Соединенных Штатов на любую(ые) иностранную(ые) заявку(и) на патент или авторское свидетельство, или с §365 (a) на любую международную заявку PCT, назначившую одну или больше стран кроме Соединенных Штатов, перечисленную(ые) ниже, а также указал ниже с расположением отметки в клетке все иностранные заявки на патент или авторское свидетельство или международную заявку PCT, поданные ранее, чем заявка, на которую предъявлено притязание на приоритет.

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

METHOD OF MARKING AND IDENTIFICATION OF ARTICLES

the specification of which is attached hereto unless the following box is checked:

09/890,846

☐ was filed on _____
as United States Application Number or PCT International Application Number
_____ and was amended on
_____ (if applicable).

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to patentability as defined in Title 37, Code of Federal Regulations, § 1.56.

I hereby claim foreign priority under Title 35, United States Code, § 119(a)-(d) or § 365(b) of any foreign application(s) for patent or inventor's certificate, or § 365(a) of any PCT International application which designated at least one country other than the United States, listed below and have also identified below, by checking the box, any foreign application for patent or inventor's certificate, or PCT International application having a filing date before that of the application on which priority is claimed.

Prior Foreign Application(s)
Прежняя(ие) иностранная(ые) заявка(и)

Притязание на приоритет не предъявляется

Priority Not Claimed

| Номер | (Number) | Страна | (Country) | День/Месяц/Год подачи (Day/Month/Year Filed) | ☐ |

| Номер | (Number) | Страна | (Country) | День/Месяц/Год подачи (Day/Month/Year Filed) | ☐ |

| Номер | (Number) | Страна | (Country) | День/Месяц/Год подачи (Day/Month/Year Filed) | ☐ |

Настоящим я предъявляю иностранные преимущественные права приоритета в соответствии с § 119 (e) раздела 35 Кодекса Соединенных Штатов на любую(ые) предварительную(ые) заявку(и), перечисленную(ые) ниже.

I hereby claim the benefit under Title 35, United States Code, § 119(e) of any United States provisional application(s) listed below.

(Заявка №)   (Дата подачи заяки)

(Application No.)   (Filing Date)

(Заявка №)   (Дата подачи заяки)

(Application No.)   (Filing Date)

Настоящим я заявляю претензию на выгоду, в соответствии с § 120 раздела 35 Кодекса Соединенных Штатов, от всех нижеперечисленных заявок(ки) США или с § 365 (с) от любой международной заявки РСТ, назначившей Соединенные Штаты, в той мере, в которой предмет изобретения в каждом пункте, на который заявлен приоритет, не был раскрыт в поданной ранее заявке США или международной заявке РСТ, как это предусмотрено в первом абзаце § 112 раздела 35 Кодекса Соединенных Штатов. Я признаю обязанность раскрыть информацию, которая является вещественной для патентоспособности, как это предусмотрено в § 1.56 раздела 37 Кодекса Федеральных Правил, которая стала доступна за период времени между подачей предшествующей заявки и датой подачи национальной или международной заявки РСТ.

I hereby claim the benefit under Title 35, United States Code, § 120 of any United States application(s), or § 365(c) of any PCT international application designating the United States, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT international application in the manner provided by the first paragraph of Title 35, United States Code, § 112, I acknowledge the duty to disclose information which is material to patentability as defined in Title 37, Code of Federal Regulations, § 1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this application.

PTO/SB/107 (3-99)
Approved for use through 9/30/99 OMB 0651-0032
Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

(Заявка №)	(Дата подачи заявки)	(Статус - запатентовано, рассматривается, заявитель отказался)
(Application No.)	(Filing Date)	(Status - patented, pending, abandoned)

(Заявка №)	(Дата подачи заявки)	(Статус - запатентовано, рассматривается, заявитель отказался)
(Application No.)	(Filing Date)	(Status - patented, pending, abandoned)

Настоящим подтверждаю, что все заявления, сделанные здесь на основе моих знаний, являются правдой, и я также верю в достоверность всех заявлений, основанных на доступной мне информации и убеждениях; кроме того, эти заявления были сделаны со знанием того, что умышленно ложные заявления и подобные им действия караются штрафом, или тюремным заключением, или тем и другим, в соответствии со статьей 1001 раздела 18 Кодекса Соединенных Штатов, и что такие ложные сведения могут сделать недействительной как эту заявку, так и любой патент, по ней выданный.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

ДОВЕРЕННОСТЬ ПОВЕРЕННОМУ: В качестве названного здесь изобретателя, я уполномочиваю следующего(их) поверенного(ых) и/или агента(ов) подать эту заявку и осуществлять все операции с ней связанные в Ведомстве по Патентам и Торговым Знакам (далее идет имя и регистрационный номер):

POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith: (list name and registration number)

Дэвид Ньюмен
Регистрационный № 30 966

David Newman
Registration No. 30,966

Send Correspondence to:

Корреспонденцию посылать по адресу:

20646 США, шт.Мэриленд, Ла Плата, Почтовый ящик 2728

CENTENNIAL SQUARE, P.O.Box 2728, LA PLATA MARYLAND 20646-2728

Direct Telephone Calls to (name and telephone number)

По телефону обращаться к:
(имя и номер телефона)
301 934 6100

(301) 934 6100

МИЩЕНКО Валентин Александрович	MISCHENKO Valentin Alexandrovich
Полное имя единственного или первого автора изобретения	Full name of sole or first inventor
	30.09.2001
Подпись автора изобретения Дата	Inventor's signature Date
Беларусь	BY
Местожительство	Residence
Беларусь	BY
Гражданство	Citizenship
220040, Беларусь, Минск, ул Некрасова 28-210	28-210, Nekrasova Str., Minsk, Belarus, 220040
Почтовый адрес	Post Office Address
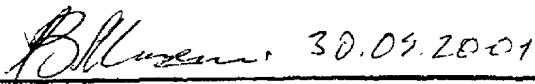
BY X

ГРИШАНОВИЧ Игорь Анатольевич	HRISHANOVICH Ihar Anatolievich
Полное имя второго автора изобретения (если имеется)	Full name of second joint inventor, if any
	30.09 2001
Подпись автора изобретения Дата	Second inventor's signature Date
Беларусь	BY
Местожительство	Residence
Беларусь	BY
Гражданство	Citizenship
220071, Беларусь, Минск, ул.Луначарского 5-39	5-39, Lunacharskogo Str., Minsk, Belarus, 220071
Почтовый адрес	Post Office Address
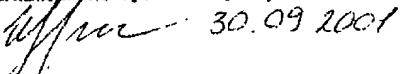
BY X

see below

(Аналогичная информация о третьем и последующих авторах изобретения должна быть представлена, а также их подписи)	(Supply information and signature for third and subsequent joint inventors.)
МИЩЕНКО Анатолий Валентинович	MISCHENKO Anatoly Valentinovich
	30 09 2001
Беларусь	Residence BY
Беларусь	Citizenship BY
220050, Беларусь, Минск, ул.Мирошниченко 5-47	Address 5-47, Miroshnichenko Str., Minsk, Belarus, 2200